IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

MONEY AND DATA PROTECTION)
LIZENZ GMBH & CO. KG,)
)
Plaintiff,)
)
v.) C.A. No. 18-1477 (CFC)
)
DUO SECURITY, INC.,)
)
Defendant.)

DUO SECURITY, INC.'S OPENING BRIEF IN SUPPORT OF ITS MOTION FOR JUDGMENT ON THE PLEADINGS OF PATENT INVALIDITY <u>UNDER 35 U.S.C. § 101</u>

MORRIS, NICHOLS, ARSHT & TUNNELL LLP
Jack B. Blumenfeld (#1014)
Jennifer Ying (#5550)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
jying@mnat.com

Attorneys for Defendant Duo Security, Inc.

OF COUNSEL:

Elizabeth Rogers Brannen
Justin M. Barnes
STRIS & MAHER LLP
725 South Figueroa Street, Suite 1830
Los Angeles, CA 90017
(213) 995-6800

October 15, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

Statutes

Rules

I. NATURE AND STAGE OF PROCEEDINGS

Money and Data Protection Lizenz GmbH & Co. KG ("MDPL") sued Duo Security, Inc. ("Duo") on September 25, 2018. D.I. 1 ("Compl."). It accused Duo of infringing U.S. Patent No. 9,246,903, titled "Authentication Method" (the " '903 Patent" or "Asserted Patent") (attached as Exhibit A to Compl., D.I. 1-1), through "products and services for two-factor authentication that perform an authentication function using a mobile device," Compl. ¶ 12. Duo moved to dismiss under Rule 12(b)(6). D.I. 9. The Court denied the motion as moot on September 4, 2019 after MDPL agreed to amend.

On September 30, 2019, MDPL filed a First Amended Complaint that continues to allege direct infringement on the basis of Duo's "products and services for two-factor user authentication that perform an authentication function using a mobile device." D.I. 15 ("Amended Complaint" or "FAC") ¶ 12. Duo answered on October 15, 2019. *See* D.I. 16. The pleadings are closed, and Duo has moved for judgment of invalidity on the pleadings pursuant to Rule 12(c) on the grounds that the subject matter claimed in the '903 Patent is ineligible for patentability under 35 U.S.C. § 101. This is Duo's opening brief in support of its motion.

II. SUMMARY OF ARGUMENT

Humans have verified identity using multiple factors for thousands of years. The Bible recounts soldiers of Gilead securing the fords of the River Jordan by requiring those seeking entry to say "shibboleth." This exposed enemy Ephraimites who might know to say the word but could not pronounce it. Since the eighteenth century, secret societies have famously used handshakes *and* passwords. For over 150 years, accessing a safety deposit box has required presenting photo identification and possessing the key. Victorian era banks used time as an additional lock safety component. Today, preschools routinely decline to release children without checking an authorization list and also placing a phone call to a parent to confirm that someone else is authorized for that day. It is thus unsurprising in the modern patent context that courts have consistently regarded the idea of authentication, "two factor" or otherwise, as abstract. *See infra* at 12-13 (collecting authorities).

The '903 Patent implements this age-old concept "in a mobile device." '903 Patent, Abstract. Users activate an authentication function for a given transaction, and the passage of time serves as one criterion for granting or denying authentication. '903 Patent, 10:39-60. The claimed invention is intended to work with conventional components, such as mobile devices of "low complexity." *Id.* at 1:54-56. The '903 Patent addresses no technical challenges. It does not improve computer functionality in any way. To the contrary, the patent claims the abstract concept of authentication using a feature left off when not in use, and which times out. The scope is indistinguishable from numerous other authentication patents that courts have correctly invalidated under *Alice Corp. Pty. Ltd. v. CLS Bank Intern.*, 573 U.S. 208 (2014) and its progeny. *See, e.g.*, *Asghari-Kamrani v. United Servs. Auto. Ass'n*, No. 2:15CV478, 2016 WL 3670804, at *4-5 (E.D. Va. July 5, 2016). There is nothing patent eligible.

III. STATEMENT OF FACTS

A. The '903 Patent Claims Authentication Using A Mobile Device.

As its title reflects, the invention of the '903 Patent is an "Authentication Method." The patent highlights the importance of verifying identity "[i]n transactions in which a user communicates with a remote transaction partner via a communication channel such as the Internet." '903 Patent at 1:15-19. It identifies several familiar transactions for which verifying identity is necessary:

> [W]hen a user makes an online bank transaction in which he identifies himself as the owner of a certain account and requests that an amount of money is remitted to some other account, an authentication method is needed for verifying the identity of the requestor. Other examples of transactions where an authentication of the user should be required are transactions in which a user

> asks for online access to a database or other online services that involve sensitive data. Another example would be a transaction for operating a door opener that provides physical access to a secure area or room.

’903 Patent at 1:19-29. “[T]he authentication function is normally inactive and is activated by the user only preliminarily for the transaction,” and then deactivated upon detection of the response from the communication channel used for authentication. ’903 Patent at 1:57-63. As a criterion for deciding whether to grant or deny authentication, the method checks whether the response is sent within a predetermined time. *Id.* at 1:3-14. The patent implicitly acknowledges that this step, too, was conventional and well-known. *See* ’903 Patent at 1:30-34 (citing authentication method of GB 2 398 159 A, attached as Exhibit 1, which provides: “The system may be adapted to cancel the transaction should no said confirmatory message be received within a predetermined period of time following transmission of said notification message.”).

The Amended Complaint alleges infringement of independent claim 1. FAC ¶ 13 (compare Compl. ¶ 13). This claim covers a method of authentication using two forms of identification: (1) a user identification sent via a first communication channel to a transaction partner from a terminal, and (2) a response that must be received within a certain time from an authentication function implemented in a mobile device, which the user activates only for the transaction. ’903 Patent at 10:39-60. In full, claim 1 reads as follows:

> A method of authenticating a user to a transaction at a terminal, comprising the steps of:
>
> transmitting a user identification from the terminal to a transaction partner via a first communication channel,
>
> providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,
>
> as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a

> predetermined time relation exists between the transmission of the user identification and a response from the second communication channel,
>
> ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,
>
> ensuring that said response from the second communication channel includes information that the authentication function is active, and
>
> thereafter ensuring that the authentication function is automatically deactivated.

’903 Patent at 10:39-60.

MDPL does not assert the remaining claims.[1] Dependent claims 2-13 expressly recite additional steps that entail similarly generic computing functionality: deactivating the authentication function after a predetermined time interval (claim 2); logging-on the mobile device to a communications network (claim 3); detecting the logged-on state and recognizing it as indicative of an active state of the authentication function (claim 4); requiring that the terminal and the mobile device satisfy a predetermined spatial relation (claims 5-8), locating the authentication device remotely from the transaction partner and limiting the information provided to the transaction partner via a third communication channel (claim 9); transmitting a password from the mobile device to the authentication function (claims 10-12); and interfacing the mobile device to an identity token, such as a smart card (claim 13). ’903 Patent at 10:63-65, 11:1-12:4. Claims 14 and 15-26, which depend from claim 14, are directed to a simple mobile device for use with the authentication method of claim 1. *Id.* at 12:5-58.

[1] To the extent that MDPL attempts to assert other claims on the grounds that the Amended Complaint identifies claim 1 as “exemplary,” the Court may treat claim 1 as representative for purposes of this motion unless MDPL establishes a basis to proceed differently (and there is none). *Cf.*, *StrikeForce Techs., Inc. v. SecureAuth Corp.*, No. LA CV-17-04314 JAK (SKx), 2017 WL 8808122, at *3-4 (C.D. Cal. Dec. 1, 2017), *aff’d,* 753 F. App’x. 914 (Fed. Cir. 2019) (treating one claim as representative of 43 asserted claims).

B. The ’903 Patent Purports To Contribute Only Simplification Through the Use of Generic Components.

The ’903 Patent acknowledges that verifying identity using a mobile device was well known. It identifies three such prior art authentication methods and does not purport to address technical problems or challenges associated with any of them. ’903 Patent at 1:30-46 (identifying GB 2 398 159 A, wherein user receives a prompt to confirm transaction on her mobile device, WO 2008/052592 A1, wherein user employs mobile device to activate and deactivate a credit card, and WO 2007/072001 A1, wherein user captures an authentication token using mobile device). There is no purported technological improvement. To the contrary, the specification touts that the claimed invention requires no specialized components or devices. ’903 Patent at 1:54-56, 2:44-46 (“It is a particular advantage of the invention that the mobile device does not have to have any specific hardware for capturing or outputting information.”) (emphasis added).

The only alleged contribution is simplicity: the invention “provide[s] an authentication method that is easy to handle” while using “mobile devices of low complexity.” ’903 Patent at 1:54-56. The patent emphasizes that this function can be accomplished using prevailing mobile networking technology. ’903 Patent at 2:44-54. The “terminal” from which a user identification is transmitted, for example, may be a cashier, a banking machine, or any other device, such as a computer. ’903 Patent at 2:36-38. The “authentication device” is merely “data processing hardware and software” that includes a database. ’903 Patent at 4:52-56. And, the mobile device may be any portable computer: “a mobile telephone or smartphone, a laptop computer, a tablet computer, or the like . . . .” ’903 Patent at 1:54-63, 2:38-43 (including those of “low complexity”). The mobile device requires only that it (1) can be activated for a certain period of time by a user for a transaction, and (2) is capable of connecting to a mobile communications network where it has an address that is linked to the identification data of the user. '903 Patent at 2:44-54.

Indeed, the Patent explains:

> [I]t is not even necessary that there is any actual communication between the authentication device and the mobile device. For example, when the mobile device has a mobile telephone (GSM) transceiver, *the activation of the authentication function may just consist of activating that transceiver, so that it connects to the nearest Base Station Subsystem (BSS) of the mobile network.* As a result, the mobile device will be identified by its device identifier (IMSI), and information on the active state of the mobile device and on the GSM-cell in which it is located will be entered into a Home Location Register (HLR) of the mobile network. Thus, the authentication device may check the active or inactive state of the mobile device just by querying the HLR.

'903 Patent at 2:54-67 (emphasis added). In other words, activating or deactivating the "authentication function" may entail simply turning on or off a mobile telephone. '903 Patent at 1:64-2:1; 2:54-67.

IV. LEGAL STANDARD

Patent eligibility presents an ultimate "question of law." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1128 (Fed. Cir. 2018); *see also CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1369 (Fed. Cir. 2011). Courts thus routinely resolve this threshold inquiry on motions to dismiss or for judgment on the pleadings. *See, e.g.*, *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1351 (Fed. Cir. 2014) (affirming grant of judgment on the pleadings pursuant to Fed. R. Civ. P. 12(c)); *see also In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 610 (Fed. Cir. 2016) (affirming dismissal pursuant to Rule 12(b)(6)); *Content Extraction and Transmission, LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1349 (Fed. Cir. 2014). Determining subject matter eligibility early in litigation may "conserve scarce judicial resources" and protect against "patents that stifle innovation and transgress the public domain." *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 718-20 (Fed. Cir. 2014) (Mayer, J., concurring), *cert. denied sub nom. Ultramercial, LLC v. WildTangent, Inc.*, 135 S. Ct. 2907 (Mem.) (2015).

Section 101 of the Patent Act sets forth the subject matter eligible to be patented. 35 U.S.C. § 101 (identifying "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof"). Although "anything under the sun that is made by man" is generally eligible, it is well-settled that "laws of nature, natural phenomena, and abstract ideas" are not. *Diamond v. Diehr*, 450 U.S. 175, 182, 185 (1981) (citations omitted); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1352–53 (Fed. Cir. 2016) (Section 101 "'contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.'") (quoting *Alice Corp. Pty. Ltd. v. CLS Bank Intern.*, 573 U.S. 208, 216 (2014)). These exceptions ensure that the "building blocks" of human ingenuity, "the basic tools of scientific and technological work," are not monopolized to impede innovation, thereby thwarting the primary purpose of patent law. *Alice*, 573 U.S. at 216 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012) and *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013)) (citing U.S. Const., Art. I, § 8, cl. 8 (Congress "shall have Power . . . To promote the Progress of Science and useful Arts")).

A two-step framework governs § 101 determinations. Courts first determine whether a patent claim is "directed to a patent-ineligible concept,"—a law of nature, natural phenomenon or abstract idea. *Alice*, 573 U.S. at 218. The exclusion of abstract ideas embodies "the longstanding rule that '[a]n idea of itself is not patentable.'" *Id.* at 216 (quoting *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)). To determine whether a claim is directed to an abstract idea at

Alice step one, the court must look at the "focus" of the claim, that is, its "character as a whole." *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1167 (Fed. Cir. 2018). For computer-related claims, the inquiry often turns on whether the claims merely "recite the performance of some business practice known from the pre-internet world" along with the instruction to perform it on a computer, or are "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *Bridge & Post, Inc. v. Verizon Commc'ns, Inc.*, ___ F. App'x. ___, 2019 WL 2896449 at *7 (Fed. Cir. Jul. 5, 2019) (quoting *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1258 (Fed. Cir. 2014)); *see Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1258 (Fed. Cir. 2017) (stating that court must "articulate with specificity what the claims are directed to" and "ask whether the claims are directed to an improvement to computer functionality versus being directed to an abstract idea").[2] Although no hard-and-fast rules define whether a claim is directed to an abstract idea, *Alice*, 573 U.S. at 221 (declining "to delimit the precise contours of the 'abstract idea' category"), the Supreme Court and the Federal Circuit have "found it sufficient to compare claims at issue to those claims already found to be directed to an abstract idea in previous cases." *Enfish*, 822 F.3d at 1334.

For claims drawn to abstract ideas, the inquiry continues. *See, e.g., Smart Authentication IP, LLC v. Electronic Arts Inc.*, No. 19-cv-01994-SI, 2019 WL 4305556, at *8 (N.D. Ca. Sept.

[2] Computer-related claims withstanding scrutiny under *Alice* step one generally recite a technological improvement in the operation of a computer. *See, e.g.*, *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018) (more accessible electronic spreadsheets); *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356 (Fed. Cir. 2018) (improved display devices); *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018) (novel method of virus scanning); *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253 (Fed. Cir. 2017) (improved computer memory system); *Thales Visionix Inc. v. United States*, 850 F.3d 1343 (Fed. Cir. 2017) (improved motion tracking system); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016) (self-referential table).

11, 2019). In *Alice* step 2, courts consider whether, alone or as "an ordered combination," the claim contains an "'inventive concept' that "'transform[s] the nature of the claim' into a patent-eligible application." 573 U.S. at 217-18. (citations omitted). Such transformation requires additional elements or features that are "'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id.* at 217-18, 221 (quoting *Mayo*, 566 U.S. at 73); *see also, e.g.*, *Bridge & Post,* 2019 WL 2896449 at *7 (affirming ineligibility where patent did "not invent a sufficiently new, non-conventional arrangement of known pieces to overcome a technical challenge"). No "inventive concept" is found if the additional elements or features are merely "well-understood, routine, conventional activities." *Alice*, 573 U.S. at 225 (quoting *Mayo*, 566 U.S. at 73).

V. ARGUMENT

The '903 Patent claims subject matter that is ineligible under § 101. The claims fail *Alice* step one because they are directed to the abstract idea of authentication. The claims fail *Alice* step two because no inventive concept transforms the abstract idea into a patent-eligible invention. The patent merely combines the age-old idea of authentication with the modern instruction to do it on a mobile phone. *See DDR Holdings*, 773 F.3d at 1257.

A. It Is Settled Law that Authentication Is An Abstract Idea.

Courts have repeatedly deemed authentication claims abstract. *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x. 1014, 1017 (Fed. Cir. 2017) (claims reciting an "authentication server" directed to "the abstract idea of providing restricted access to resources"); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372-73 (Fed. Cir. 2011) (authentication based on past transaction and internet address); *Telesign Corp. v. Twilio, Inc.*, No. 3:18-cv-03279 (VC), D.I. 219 (N.D. Cal. Oct. 19, 2018) (authentication using passcodes) (Ex. 2); *StrikeForce Techs.*, 2017 WL 8808122, at *6 (authentication using multiple communication channels);

Asghari-Kamrani, 2016 WL 3670804, at *4-5 (authentication using a dynamic code); *GoDaddy.com LLC v. RPost Commc'ns Ltd.*, No. CV-14-00126-PHX-JAT, 2016 WL 3165536, at *7 (D. Ariz. June 7, 2016), *aff'd*, 685 F. App'x 992 (Fed. Cir. 2017) (authentication using third-party intermediary); *OpenTV, Inc. v. Apple Inc.*, No. 5:15-cv-02008-EJD, 2016 WL 344845, a *5 (N.D. Cal. Jan. 28, 2016) (authentication to deliver digital content); *Kinglite Holdings Inc. v. Micro-Star Int'l Co.*, No. CV1403009JVS(PJWx), 2015 WL 6437836, at *8 (C.D. Cal. Oct. 16, 2015) (authentication of request using further abstractions).

Use of a mobile device does not change the analysis. *See e.g.*, *Consumer 2.0, Inc. v. Tenant Turner, Inc.*, 343 F. Supp. 3d 581, 588 (E.D. Va. 2018) (authentication using mobile device to provide automated access to property directed to patent ineligible abstract idea); *Bytemark, Inc. v. Masabi Ltd.*, No. 216CV00543-JRG-RSP, 2018 WL 7272023, at *8 (E.D. Tex. Nov. 26, 2018) (same for authentication of electronic tickets using mobile device).

Neither does the time-out feature. *See Asghari-Kamrani*, 2016 WL 3670804, at *2; *see also BlackBerry Ltd. v. Facebook, Inc.*, No. CV 18-1844 GW(KSx), 2018 WL 4847053, at *10 (C.D. Cal. Aug. 21, 2018) (method of displaying timestamp based on whether a predetermined duration of time has passed claimed ineligible abstract idea); *Image Processing Techs., LLC v. Samsung Elecs. Co.*, No. 2:16-CV-00505-JRG, 2017 WL 10185856, at *1 (E.D. Tex. Oct. 24, 2017) (method that included determining whether data satisfied a "predetermined time coincidence criteria" drawn to ineligible abstract idea); *CalAmp Wireless Networks Corp. v. ORBCOMM, Inc.*, 233 F. Supp. 3d 509, 515 (E.D. Va. 2017) (claims to device capable of determining whether an article is within a spatial zone during a predetermined time lacked inventive concept); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093, 1095 (Fed. Cir. 2016) (claims disclosing ways to detect fraud and misuse by identifying accesses to sensitive information during a pre-determined time interval drawn to ineligible abstract idea); *Adrea, LLC v. Barnes & Noble, Inc.*, 13-CV-4137 (JSR), 2015 WL 4610465, at *5 (S.D.N.Y. July 24, 2015) (claims directed to method for restricting access to electronic books by associating a predetermined amount of time after electronic book is stored on viewer ineligible; associating predetermined amount of time is a "conventional and quotidian" task).

B. The '903 Patent Claims Are Drawn To The Abstract Idea Of Authentication.

The focus and character of the '903 Patent claims is authentication. The specification makes clear that the purpose of the claimed invention is to authenticate users to a transaction. '903 Patent at 1:54-56. There is no meaningful difference from the claims held ineligible in *StrikeForce Techs.*, 2017 WL 8808122, at *1, and *Asghari-Kamrani*, 2016 WL 3670804, at *1, as directed to the abstract idea of user authentication.

The patent in *StrikeForce Technologies* was directed to "multichannel security systems and methods for authenticating a user seeking to gain access to a secure network," such as an online bank. 2017 WL 8808122, at *1 and 3-4 (quoting representative claim to "method for employing a multichannel security system to control access to a computer" that recited steps including "*receiving in a first channel a login identification* demand to access a host computer also in the first channel," "*receiving at a security computer in a second channel the demand for access and the login identification*," comparing the transmitted data, and depending on the comparison "outputting an instruction" to grant or deny access) (emphasis added). At *Alice* step one, the district court concluded that the asserted claims address the abstract idea of providing restricted access to resources. *Id.* at *6. The court reasoned that the asserted claims address a long-established means of transmitting sensitive information and were not specifically directed to an improvement in computer functionality. The claims simply applied established, noncomputer-based methods for transmitting, processing and authenticating sensitive data in the context of the use of computers connected to the internet. *Id.* The same is true here. *See* '903 Patent at 10:41-46. ("[T]ransmitting a user identification . . . via a first communication channel" and "providing an authentication step … us[ing] a second communication channel").

The time-sensitive authentication function held ineligible in *Asghari-Kamrani* is similarly instructive. There, the claims specified a series of steps, including: (1) receiving a request for a dynamic code during a transaction; (2) generating a dynamic, non-predictable, and time-dependent code, wherein the dynamic code is invalid after being used; (3) providing the generated dynamic code to the user; (4) receiving a request to authenticate the user; and (5) authenticating the user and communicating the result). 2016 WL 3670804 at *2. The court held that these claims were directed to a "the abstract idea of using a third party and a random, time-sensitive code to confirm the identity of a participant to a transaction." *Id.* at *4 (emphasis added).

Both the dynamic code in *Asghari-Kamrani* and the authentication function of the '903 Patent are time-sensitive, and activated by a user only for a transaction. *See* '903 Patent at 10:3-65. As the court recognized in *Asghari-Kamrani*, use of a temporary code narrows the claims cover to a more specific concept of authentication, but the claims remain abstract. 2016 WL 3670804 at *4 ("the abstract idea of using a third party and a random, time-sensitive code to confirm the identity of a participant to a transaction"). A narrower abstract idea is nevertheless ineligible for patentability. *Cf. Mayo*, 566 U.S. at 88-89 ("[O]ur cases have not distinguished among different laws of nature according to whether or not the principles they embody are sufficiently narrow") (citing *Parker v. Flook*, 437 U.S. 584 (1978) (holding narrow mathematical formula unpatentable). The claims of the '903 Patent are just as abstract, and indeed almost identical in all pertinent respects to the claims held ineligible in *Asghari-Kamrani*.

Like the claims recognized as abstract in *StrikeForce Technologies* and *Asghari-Kamrani*, the asserted claims of the '903 Patent neither address a problem rooted in technology, nor aim to improve computer functionality. Authentication itself is not a problem rooted in technology, and including a rudimentary mobile device cannot save the claims from abstraction. *See also, e.g.*, *Consumer 2.0*, 343 F. Supp. 3d at 594 (claims using generic computing devices and techniques to provide automated entry to property held abstract); *Network Apparel Grp., LP v. Airwave Networks Inc.*, 154 F. Supp. 3d 467, 490 (W.D. Tex. 2015), *report and recommendation adopted*, No. 6:15-CV-00134, 2016 WL 4718428 (W.D. Tex. Mar. 30, 2016), *aff'd*, 680 F. App'x 1003 (Fed. Cir. 2017) (finding that authenticating a particular network device identified by its unique attribute is a well-understood, routine, conventional activity in the computer networking field).[3] The invention claimed here simply authenticates a user to a transaction using conventional technology in conventional ways. *See, e.g., Smart Authentication*, 2019 WL 4305556, at *7.

It is directed to an ineligible abstract idea, and as shown next, there is no "'inventive concept' sufficient to 'transform' the claimed abstract idea into patent-eligible application." *Alice*, 573 U.S. at 221.

[3] In stark contrast to claims found eligible, the '903 Patent does not purport to perform authentication in any novel or unusual manner or to contribute any improvement to the technological landscape. *Cf. Universal Secure Registry, LLC v. Apple Inc.*, No. 17-585-CFC-SRF, 2018 WL 4502062, at *11 (D. Del. Sept. 19, 2018) (finding that authentication method using a mobile device was not drawn to an abstract idea where the patent was directed to "an improvement in the security of mobile devices by using a biometric sensor, a user interface, a communication interface, and a processor working together to generate a time varying or other type of code that can be used for a single transaction, preventing the merchant from retaining identifying information that could be fraudulently used in subsequent transactions").

C. The Asserted Claims Lack An Inventive Concept.

Taken both individually and as an ordered combination, the ’903 Patent claims recite no additional elements or features that amount to something patentable. As in *Bridge & Post*, the ’903 Patent acknowledges that its means of carrying out authentication are well-known. 2019 WL 2896449 at *7 (holding that claim fails *Alice* step two “as evidenced by its acknowledgement that [its abstract concept] was known in the pre-Internet world, and that its steps for accomplishing this on the Internet were conventional”). Here too, the claims use conventional computing components in routine ways. They amount to no more than an attempt to patent the ineligible concept itself.

1. Each Element is Conventional.

Asserted claim 1 identifies a method using the following elements: a terminal, an authentication device, and a mobile device. As the specification makes clear, these elements are all generic computer components. ’903 Patent at 2:35-49; 4:53-56. To wit:

- The “terminal” is a cashier or any device, such as a computer. ’903 Patent at 2:35-38.
- The authentication device is “formed by data processing hardware and software and includes a database…” *Id.* at 4:53-56.
- The mobile device is a mobile telephone, a smartphone, a laptop computer, a tablet computer, or any device “capable of connecting to a mobile communications network” *Id.* at 2:45-49.

Computers, databases, and mobile devices are well-known, generic components. *Alice*, 573 U.S. at 223-24 (“Given the ubiquity of computers . . . wholly generic computer implementation is not generally the sort of additional feature that provides any practical assurance that the process is more than a drafting effort designed to monopolize the abstract idea itself.”) (internal quotation marks and citations omitted); *Prism Techs.,* 696 F. Appx. at 1017 ("authentication server," "access server," "and "database" are generic components); *Joao Bock Transaction Sys., LLC v. Jack Henry & Assocs., Inc.*, 76 F. Supp. 3d 513, 522 (D. Del. 2014), *aff'd*, 803 F.3d 667 (Fed. Cir. 2015) (addition of well-known data processing software is not transformative). The specification acknowledges as much, identifying these components as elements of prior art authentication methods. *See* '903 Patent at 1:30-46 ("GB 2398 159 A discloses an authentication method of the type indicated above, wherein the *authentication function* prompts the user to confirm the transaction, and a corresponding confirmation signal is sent from the *mobile device* to the *authentication device*.") (emphasis added).

The remaining claims recite either no additional components or components that are equally generic. *See* '903 Patent claims 2 (automatic deactivation after predetermined time); 3 (mobile communications network provides second communication channel); 4 (authentication device detects logged-on state of mobile device on communications network); 5-8 (use of mobile device location); 10-12 (transmitting, storing, generating, and/or converting a password); 13 (interfacing to an identity token of user); 14 (mobile device comprising wireless transceiver, ON-switch, and electronic controller); 15 (rechargeable battery); 16 (display indicating battery charge state); 17-18 (connectors); 19 (wireless detection of device position); 20 ("authentication function consists only of activating and deactivating the transceiver"); 21 (device that encapsulates and prevents access to controller); 22 (self-destruction function); 23 (transceiver constitutes an only data input and output port of controller); 24-25 (device stores plurality of mobile addresses); 26 ("acoustic transducer," e.g., "a buzzer," per 8:49-52 & FIG. 9).

2. The Claims Use Conventional Elements in Conventional Ways.

Claim 1 recites the use of computers, databases, and mobile devices according to their conventional functions. Essentially, the claimed computer, database, and mobile device do nothing more than send, receive, store, and verify information. *See* ’903 Patent at 10:49-52. Such conventional computing functions do not constitute an inventive concept. *See e.g. Bytemark*, 2018 WL 7272023, at *6 (sending, receiving, storing, and verifying information constitute conventional functions of computers, servers, and devices); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016) (claim elements “insufficient to pass the test of an inventive concept in the application” where “[n]othing in the claims, understood in light of the specification, requires anything other than off-the-shelf, conventional computer, network, and display technology for gathering, sending, and presenting the desired information); *Asghari-Kamrani*, 2016 WL 3670804, at *5 (sending data electronically and comparing the data to see if they are the same describes conventional computer functions); *see also Smart Sys. Innovations, LLC v. Chicago Transit Auth.*, 873 F.3d 1364, 1372 (Fed. Cir. 2017) ([C]laims directed to the collection, storage, and recognition of data are directed to an abstract idea).

Similarly, the steps and features of the additional claims cover well-understood, routine activities. For example, dependent claims 5-8 recite using the geographic location of an individual’s mobile device to verify identity data. ‘903 Patent at 11:5-35. Again, the claims merely implement the abstract idea of authentication using fundamental aspects of prevailing technology, here location based services of mobile communication networks. *Id.* Such conventional communication means is not inventive. *See, e.g.*, *Front Row Techs., LLC v. NBA Media Ventures, LLC*, 204 F. Supp. 3d 1190, 1266-68, 1280-1281 (D.N.M. 2016), *aff’d sub nom. Front Row Techs. LLC v. MLB Advanced Media, L.P.*, 697 F. App’x 701 (Fed. Cir. 2017) (finding that claim describing a method that: (i) determines a handheld device user’s location; and (ii) authorizes devices within a certain geographic area to receive streaming video was drawn to ineligible abstract idea and contained no inventive concept); *British Telecommunications plc* *v. IAC/InterActiveCorp*, 381 F. Supp. 3d 293, 307-11 (D. Del. 2019) (finding no inventive concept where invention for generating information based on user location used conventional communication means).

3. The Ordered Combination Adds Nothing.

Taken as an ordered combination, the elements of the claims are no more transformative. Rather, the claims proceed logically from the concept of providing access to restricted resources by verifying the identity of a user to a transaction. The claims entail two basic steps: (1) transmitting user identification via a first communication channel, and (2) authenticating the user by sending and receiving information to and from the user's mobile device via a second communication channel. '903 Patent at 10:41-60 (describing only transmitting identification data and providing an authentication step). There is also activation and a time-out feature that cause the claims to sweep less expansively without fundamentally transforming the purported innovation.

These ordered steps reflect processes that courts have held to be too routine and conventional to provide an inventive concept. *See e.g.*, *StrikeForce Techs.*, 2017 WL 8808122, at *6 ("[T]he 'ordered combination' on which Plaintiff relies is nothing more than an obvious and logical structure for the step-by-step process for sending and receiving information through a system that has an authenticating feature."); *Telesign Corp.*, 3:18-cv-3279-VC, D.I. 219, slip op. at 1-3 (process of verifying the identity of a person by sending codes through electronic contacts and then verifying the person's identity using a pre-cleared contact proceeded logically from the basic premise of using information to verify a user's identity); *Asghari-Kamrani*, 2016 WL 3670804, at *5 ("Considered as an ordered combination, the claim elements do not add anything inventive to the abstract concept underlying them. They simply instruct a generic computer or computers to verify the identity of a participant to a transaction using a randomly generated code."); *Network Apparel Grp.*, 154 F. Supp. 3d at 490 (authentication step as "a well-understood, routine, conventional activity in the computer networking field that does not make the claim patent-eligible").

In sum, the '903 Patent claims are drawn to the abstract idea of authentication. The aim of the patent is simplicity. It lacks any inventive concept. The claims use conventional components in the most conventional of ways and are not directed to eligible subject matter.

VI. CONCLUSION

For the foregoing reasons, Duo respectfully requests a judgment invalidating the claims of the '903 Patent under 35 U.S.C. § 101 and dismissing MDPL's Amended Complaint.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jack B. Blumenfeld

Jack B. Blumenfeld (#1014)
Jennifer Ying (#5550)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
jying@mnat.com

Attorneys for Defendant Duo Security, Inc.

OF COUNSEL:

Elizabeth Rogers Brannen
Justin M. Barnes
STRIS & MAHER LLP
725 South Figueroa Street, Suite 1830
Los Angeles, CA 90017
(213) 995-6800

October 15, 2019

CERTIFICATE OF SERVICE

I hereby certify that on October 15, 2019, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on October 15, 2019, upon the following in the manner indicated:

David E. Moore, Esquire *VIA ELECTRONIC MAIL*
Bindu A. Palapura, Esquire
Stephanie E. O'Byrne, Esquire
POTTER, ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 North Market Street
Wilmington, DE 19801
Attorneys for Plaintiff

Scott T. Weingaertner, Esquire *VIA ELECTRONIC MAIL*
Stefan Mentzer, Esquire
Leon Miniovich, Esquire
WHITE & CASE LLP
1221 Avenue of the Americas
New York, NY 10020
Attorneys for Plaintiff

/s/ Jack B. Blumenfeld

Jack B. Blumenfeld (#1014)